Atty. Dkt. No. 040405/0326

JC864 U.S. PTO 09/645588 08/25/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#2 Priority Paper MA 10/20/00

Applicant: Seigo ARITA

Title: SECURE PARAMETER GENERATING DEVICE AND PARAMETER GENERATING METHOD IN ALGEBRAIC CURVE CRYPTOGRAPHY

Appl. No.: Unassigned

Filing Date: 8/25/2000

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japan Patent Application No. 11-242075 filed 8/27/1999.

Respectfully submitted,

Date August 25, 2000

By Phillip J. Articola Reg. No. 38,819

for / David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

002.379415.1

40405/325
Seigo ARITA

JC864 U.S. PTO
09/645588
08/25/00

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 1999年 8月27日

出願番号
Application Number: 平成11年特許願第242075号

出願人
Applicant (s): 日本電気株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

2000年 6月 9日

特許庁長官
Commissioner,
Patent Office

近藤隆彦

特許庁長官印

出証番号　出証特2000－3044421

【書類名】　特許願
【整理番号】　33509589
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
H04L　9/06
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　有田　正剛
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100082935
【弁理士】
【氏名又は名称】　京本　直樹
【電話番号】　03-3454-1111
【選任した代理人】
【識別番号】　100082924
【弁理士】
【氏名又は名称】　福田　修一
【電話番号】　03-3454-1111
【選任した代理人】
【識別番号】　100085268
【弁理士】
【氏名又は名称】　河合　信明
【電話番号】　03-3454-1111
【手数料の表示】
【予納台帳番号】　008279

【納付金額】　　　21,000円

【提出物件の目録】

【物件名】　　　明細書　1

【物件名】　　　図面　1

【物件名】　　　要約書　1

【包括委任状番号】　9115699

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　代数曲線暗号における安全なパラメータの生成装置、生成方法、および記録媒体

【特許請求の範囲】

【請求項１】

（ａ）曲線の複雑さの度合いを指定する2つの異なる素数a、b、および、使用したい暗号鍵のサイズnを入力する入力装置と、

（ｂ）前記入力手段に入力された素数a、素数b、暗号鍵のサイズnをそれぞれ記憶するa記憶手段、b記憶手段、および、n記憶手段と、

（ｃ）前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算装置と、

（ｄ）前記スティッケルバーガー要素計算装置により演算されたスティッケルバーガー要素ωを記憶するω記憶手段と、

（ｅ）前記a記憶手段、前記b記憶手段、前記n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算装置と、

（ｆ）前記ヤコビ和候補値計算装置により演算された素数p、ヤコビ和候補値jをそれぞれ記憶するp記憶手段、およびj記憶手段と、

（ｇ）前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、素数b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算装置と、

（ｈ）前記位数候補値計算装置により演算された集合Hを記憶するH記憶手段と、

（ｉ）前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定装置と、

（ｊ）前記安全性判定装置により検索された候補値hを記憶するh記憶手段と、

（ｋ）前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定され

る代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定装置と、

前記パラメータ決定装置で演算された代数曲線のパラメータを出力する出力装置と、

を備えたことを特徴とする代数曲線暗号における安全なパラメータの生成装置。

【請求項２】　前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、式$\omega = \Sigma_t$ [<t/a> + <t/b>] σ_{$-t^{-1}$}（tはabを法とする既約剰余類の代表系を走り、[λ]は有理数λを超えない最大の整数を表し、<λ>は有理数λの小数部分λ-[λ]を表し、σ_tは円のab分体におけるガロア写像$\xi \rightarrow \xi^t$を表す(ξは1の原始ab乗根)）を用いてスティッケルバーガー要素ωを演算する前記スティッケルバーガー要素計算装置を備えることを特徴とする請求項１記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項３】　前記a記憶手段、前記b記憶手段、前記n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、１の原始ab乗根で生成される円分体Kの素イデアルを生成する代数的整数γで、その絶対ノルムが2n/(a-1)(b-1)程度のビット長の素数pとなるαをランダムに生成し、式$j = \gamma^{\omega}$を用いてヤコビ和候補値jを演算する前記ヤコビ和候補値計算装置を備えることを特徴とする請求項１または２記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項４】　前記a記憶手段、前記b記憶手段、前記j記憶手段からそれぞれ素数a、素数b、ヤコビ和候補値jを取得し、１以上2ab以下の整数である各kに対して、ξを１の原始ab乗根とするとき、式 $h_k = \mathrm{Norm}_{K|Q}(1 + (-\xi)^k\ j)$（Norm_{K|Q}は、円のab分体Kにおけるノルム写像）を用いて、パラメータa、bで指定される代数曲線のヤコビアン群の位数の候補値h_kを演算し、候補値の集合H={h_1、h_2、．．．．、h_{2ab}}を演算する前記位数候補値計算装置を備えることを特徴とする請求項１、２、または３記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項５】　前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数pを法とする１

の原始a乗根ζ_aおよび１の原始b乗根ζ_bを求め、１以上a以下の各整数l、および１以上b以下の各整数mに対して、式$\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$で定義される代数曲線上のランダムな点Gを生成し、点Gの表すヤコビアン群における要素のh倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数a、素数bで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータとしてp、ζ_a^lおよびζ_b^mを出力する前記パラメータ決定装置を備えることを特徴とする請求項１、２、３または４記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項６】

（ａ）a記憶手段、b記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数a、bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算手順と、

（ｂ）前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素ωをω記憶手段に記憶する手順と、

（ｃ）前記a記憶手段、前記b記憶手段、n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

（ｄ）前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶手段、およびj記憶手段に記憶する手順と、

（ｅ）前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、素数b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

（ｆ）前記位数候補値計算手順により演算された集合HをH記憶手段に記憶する手順と、

（ｇ）前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

（ｈ）前記安全性判定手順により検索された候補値hをh記憶手段に記憶する手順と、

（ｉ）前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

を含むことを特徴とする代数曲線暗号における安全なパラメータの生成方法。

【請求項７】　前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、式$\omega = \Sigma_t$ [<t/a> + <t/b>] σ_{-t^{-1}}（tはabを法とする既約剰余類の代表系を走り、[λ]は有理数λを超えない最大の整数を表し、<λ>は有理数λの小数部分λ-[λ]を表し、σ_tは円のab分体におけるガロア写像$\zeta \rightarrow \zeta^t$を表す($\zeta$は1の原始ab乗根)）を用いてスティッケルバーガー要素ωを演算する前記スティッケルバーガー要素計算手順を含むことを特徴とする請求項６記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項８】　前記a記憶手段、前記b記憶手段、前記n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、１の原始ab乗根で生成される円分体Kの素イデアルを生成する代数的整数γで、その絶対ノルムが2n/(a-1)(b-1)程度のビット長の素数pとなるαをランダムに生成し、式$j = \gamma^{\omega}$を用いてヤコビ和候補値jを演算する前記ヤコビ和候補値計算手順を含むことを特徴とする請求項６または７記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項９】　前記a記憶手段、前記b記憶手段、前記j記憶手段からそれぞれ素数a、素数b、ヤコビ和候補値jを取得し、１以上2ab以下の整数である各kに対して、ζを１の原始ab乗根とするとき、式 $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$（Norm_{K|Q}は、円のab分体Kにおけるノルム写像）を用いて、パラメータa、bで指定される代数曲線のヤコビアン群の位数の候補値h_kを演算し、候補値の集合H={h_1、h_2、．．．．、h_{2ab}}を演算する前記位数候補値計算手順を含むことを特徴とする請求項６、７、または８記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項１０】　前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数pを法とする

１の原始a乗根ζ_aおよび１の原始b乗根ζ_bを求め、１以上a以下の各整数l、および１以上b以下の各整数mに対して、式$\zeta_a^{\,l}Y^a+\zeta_b^{\,m}X^b+1=0$で定義される代数曲線上のランダムな点Gを生成し、点Gの表すヤコビアン群における要素のh倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数a、素数bで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータとしてp、$\zeta_a^{\,l}$および$\zeta_b^{\,m}$を出力する前記パラメータ決定手順を含むことを特徴とする請求項６、７、８または９記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項１１】

（ａ）a記憶手段、b記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数a、bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算手順と、

（ｂ）前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素ωをω記憶手段に記憶する手順と、

（ｃ）前記a記憶手段、前記b記憶手段、n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

（ｄ）前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶手段、およびj記憶手段に記憶する手順と、

（ｅ）前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、記憶手段b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

（ｆ）前記位数候補値計算手順により演算された集合HをH記憶手段に記憶する手順と、

（ｇ）前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

（ｈ）前記安全性判定手順により検索された候補値hをh記憶手段に記憶する手順

と、

（ｉ）前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

をコンピュータに実行させるプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、離散対数型暗号（以下、代数曲線暗号と記す）における安全なパラメータの生成装置、生成方法、および記録媒体に関し、特に、代数曲線のヤコビアン群を用いた離散対数型暗号における安全なパラメータの生成装置、生成方法、および記録媒体に関する。

【０００２】

【従来の技術】

離散対数型暗号は、与えられた有限群上の離散対数問題の困難性に基づく公開鍵暗号方式である。暗号の安全性を保つためには、用いる有限群の位数は、ほぼ素数、すなわち、小さな整数と大きな素数の積でなければならない。離散対数型暗号の一種である代数曲線暗号では、ヤコビアン群の位数がほぼ素数である代数曲線を用いる必要がある。

【０００３】

最も簡単な代数曲線である楕円曲線の場合には、任意の楕円曲線に対して、そのヤコビアン群の位数を計算する効率的なアルゴリズムが知られている。例えば、1995年、レネ＝スクーフ著、カウンティング＝ポインツ＝オン＝エリプティック＝カーブズ＝オーバー＝ファイナイト＝フィールズ、ジャーナル＝ドゥ＝セオリ＝ドゥ＝ノンブル、7巻、219-254（Rene Schoof、Counting points on elliptic curves over finite fields、Journal de Theorie des Nombres、de Bordeaux 7 (1995)、219-254、Institue deMathematique de Bordeaux）に詳しい記述がある。ヤコビアン群の位数がほぼ素数である楕円曲線を得るには、上記のアルゴ

リズムを利用して、以下のようにすればよい。

【０００４】

1。ランダムな楕円曲線Eを生成する。

2。Eのヤコビアン群の位数nを計算する。

3。nがほぼ素数ならばEを出力し、そうでないならば1に戻る。

【０００５】

楕円曲線以外の代数曲線の場合には、例外的な一部の超楕円曲線を除いて、そのヤコビアン群の位数を計算する効率的なアルゴリズムは知られていない。そのため、代数曲線暗号で使用できる代数曲線は、楕円曲線および例外的な一部の超楕円曲線に限定されてしまう。

【０００６】

また、ヤコビアン群における要素のh倍演算に関しては、「有田、吉川、宮内、C_{ab}曲線を用いた離散対数型暗号のソフトウェア実装、1999年暗号と情報セキュリティシンポジウム、pp.573-578」が知られている。

【０００７】

また、「特開平６－２８２２２６号公報」記載の技術は、「任意の素数を選び、素数に対応した暗号化鍵を公開ファイル装置に登録し、素数、暗号鍵に対応する復号鍵表により生成し、素数と共に復号鍵表を復号装置に記憶しておき、暗号化装置が公開ファイル装置より受信者（復号装置）の公開鍵を入手し、平文を楕円曲線上で乗算し、その値を暗号文として復号装置に送信し、復号装置が暗号文から楕円曲線のパラメータを計算し、復号鍵表を用いてパラメータに対応する復号鍵を選び、暗号文を楕円曲線で乗算した値から中国剰余定理を用いて平文を得る」ものである。

【０００８】

【発明が解決しようとする課題】

上述した従来技術においては、使用できる代数曲線が、楕円曲線および例外的な一部の超楕円曲線に限定されている。楕円曲線および超楕円曲線は、代数曲線全体から見ると、極めて特殊な代数曲線であり、暗号解読のためのターゲットが狭くなるため、代数曲線暗号の安全性に問題がある。

【０００９】

本発明の目的は、従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることを可能とし、代数曲線暗号の安全性を向上させることである。

【００１０】

【課題を解決するための手段】

本発明の第１の代数曲線暗号における安全なパラメータの生成装置は、

（ａ）曲線の複雑さの度合いを指定する2つの異なる素数a、b、および、使用したい暗号鍵のサイズnを入力する入力装置と、

（ｂ）前記入力手段に入力された素数a、素数b、暗号鍵のサイズnをそれぞれ記憶するa記憶手段、b記憶手段、および、n記憶手段と、

（ｃ）前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算装置と、

（ｄ）前記スティッケルバーガー要素計算装置により演算されたスティッケルバーガー要素ωを記憶するω記憶手段と、

（ｅ）前記a記憶手段、前記b記憶手段、前記n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算装置と、

（ｆ）前記ヤコビ和候補値計算装置により演算された素数p、ヤコビ和候補値jをそれぞれ記憶するp記憶手段、およびj記憶手段と、

（ｇ）前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、素数b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算装置と、

（ｈ）前記位数候補値計算装置により演算された集合Hを記憶するH記憶手段と、

（ｉ）前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定装置と、

（ｊ）前記安全性判定装置により検索された候補値hを記憶するh記憶手段と、

（ｋ）前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれ

ぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定装置と、
前記パラメータ決定装置で演算された代数曲線のパラメータを出力する出力装置と、
を備える。

【００１１】

本発明の第２の代数曲線暗号における安全なパラメータの生成装置は、前記第１の代数曲線暗号における安全なパラメータの生成装置であって、
前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、式$\omega = \Sigma_t$ [<t/a> + <t/b>] σ_{$-t^{-1}$}（tはabを法とする既約剰余類の代表系を走り、[λ]は有理数λを超えない最大の整数を表し、<λ>は有理数λの小数部分λ-[λ]を表し、σ_tは円のab分体におけるガロア写像$\zeta \rightarrow \zeta^t$を表す(ζは1の原始ab乗根)）を用いてスティッケルバーガー要素ωを演算する前記スティッケルバーガー要素計算装置を備える。

【００１２】

本発明の第３の代数曲線暗号における安全なパラメータの生成装置は、前記第１、または第２の代数曲線暗号における安全なパラメータの生成装置であって、
前記a記憶手段、前記b記憶手段、前記n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、１の原始ab乗根で生成される円分体Kの素イデアルを生成する代数的整数γで、その絶対ノルムが2n/(a-1)(b-1)程度のビット長の素数pとなるαをランダムに生成し、式$j = \gamma^{\omega}$を用いてヤコビ和候補値jを演算する前記ヤコビ和候補値計算装置を備える。

【００１３】

本発明の第４の代数曲線暗号における安全なパラメータの生成装置は、前記第１、第２、または第３の代数曲線暗号における安全なパラメータの生成装置であって、前記a記憶手段、前記b記憶手段、前記j記憶手段からそれぞれ素数a、素数b、ヤコビ和候補値jを取得し、１以上2ab以下の整数である各kに対して、ζを１

の原始ab乗根とするとき、式 $h_k = Norm_{K|Q}(1+(-\zeta)^k j)$（Norm_{K|Q}は、円のab分体Kにおけるノルム写像）を用いて、パラメータa、bで指定される代数曲線のヤコビアン群の位数の候補値h_kを演算し、候補値の集合H={h_1、h_2、．．．、h_{2ab}}を演算する前記位数候補値計算装置を備える。

【００１４】

本発明の第５の代数曲線暗号における安全なパラメータの生成装置は、前記第１、第２、第３、または第４の代数曲線暗号における安全なパラメータの生成装置であって、前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数pを法とする１の原始a乗根ζ_aおよび１の原始b乗根ζ_bを求め、１以上a以下の各整数l、および１以上b以下の各整数mに対して、式$\zeta_a^{l} Y^a + \zeta_b^{m} X^b + 1 = 0$で定義される代数曲線上のランダムな点Gを生成し、点Gの表すヤコビアン群における要素のh倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数a、素数bで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータとしてp、ζ_a^{l}およびζ_b^{m}を出力する前記パラメータ決定装置を備える。

【００１５】

本発明の第１の代数曲線暗号における安全なパラメータの生成方法は、

（ａ）a記憶手段、b記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数a、bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算手順と、

（ｂ）前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素ωをω記憶手段に記憶する手順と、

（ｃ）前記a記憶手段、前記b記憶手段、n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

（ｄ）前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶手段、およびj記憶手段に記憶する手順と、

（ｅ）前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、素

数b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

（ｆ）前記位数候補値計算手順により演算された集合HをH記憶手段に記憶する手順と、

（ｇ）前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

（ｈ）前記安全性判定手順により検索された候補値hをh記憶手段に記憶する手順と、

（ｉ）前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

を含む。

【００１６】

本発明の第２の代数曲線暗号における安全なパラメータの生成方法は、前記第１の代数曲線暗号における安全なパラメータの生成方法であって、前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、式$\omega = \Sigma_t [\langle t/a\rangle + \langle t/b\rangle] \sigma_{\{-t^{-1}\}}$（tはabを法とする既約剰余類の代表系を走り、［λ］は有理数λを超えない最大の整数を表し、$\langle\lambda\rangle$は有理数λの小数部分λ－［λ］を表し、σ_tは円のab分体におけるガロア写像$\zeta \rightarrow \zeta^t$を表す（ζは1の原始ab乗根））を用いてスティッケルバーガー要素ωを演算する前記スティッケルバーガー要素計算手順を含む。

【００１７】

本発明の第３の代数曲線暗号における安全なパラメータの生成方法は、前記第１、または第２の代数曲線暗号における安全なパラメータの生成方法であって、前記a記憶手段、前記b記憶手段、前記n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、１の原始ab乗根で生成される円分体Kの素イデアルを生成する代数的整数γで、その絶対ノルムが2n/(a-1)(b-1)程度のビット長の素数pとなるαをランダムに生成し

、式$j = \gamma^{\omega}$を用いてヤコビ和候補値jを演算する前記ヤコビ和候補値計算手順を含む。

【００１８】

本発明の第４の代数曲線暗号における安全なパラメータの生成方法は、前記第１、第２、または第３の代数曲線暗号における安全なパラメータの生成方法であって、前記a記憶手段、前記b記憶手段、前記j記憶手段からそれぞれ素数a、素数b、ヤコビ和候補値jを取得し、１以上2ab以下の整数である各kに対して、ζを１の原始ab乗根とするとき、式 $h_k = Norm_{K|Q}(1+(-\zeta)^k j)$（Norm_{K|Q}は、円のab分体Kにおけるノルム写像）を用いて、パラメータa、bで指定される代数曲線のヤコビアン群の位数の候補値h_kを演算し、候補値の集合$H=\{h_1、h_2、...、h_{2ab}\}$を演算する前記位数候補値計算手順を含む。

【００１９】

本発明の第５の代数曲線暗号における安全なパラメータの生成方法は、前記第１、第２、第３、または第４の代数曲線暗号における安全なパラメータの生成方法であって、前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数pを法とする１の原始a乗根ζ_aおよび１の原始b乗根ζ_bを求め、１以上a以下の各整数l、および１以上b以下の各整数mに対して、式$\zeta_a^{\,l} Y^a + \zeta_b^{\,m} X^b + 1 = 0$で定義される代数曲線上のランダムな点Gを生成し、点Gの表すヤコビアン群における要素のh倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数a、素数bで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータとしてp、$\zeta_a^{\,l}$および$\zeta_b^{\,m}$を出力する前記パラメータ決定手順を含む。

【００２０】

本発明の記録媒体は、

（ａ）a記憶手段、b記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数a、bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算手順と、

（ｂ）前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素ωをω記憶手段に記憶する手順と、

（ｃ）前記a記憶手段、前記b記憶手段、n記憶手段、前記ω記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

（ｄ）前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶手段、およびj記憶手段に記憶する手順と、

（ｅ）前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、記憶手段b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

（ｆ）前記位数候補値計算手順により演算された集合HをH記憶手段に記憶する手順と、

（ｇ）前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

（ｈ）前記安全性判定手順により検索された候補値hをh記憶手段に記憶する手順と、

（ｉ）前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

をコンピュータに実行させるプログラムを記録する。

【００２１】

【発明の実施の形態】

まず、本発明の原理について説明する。

【００２２】

本発明は、$\alpha Y^a + \beta X^b + 1 = 0$という形の定義方程式をもつ代数曲線のクラスから、そのヤコビアン群の位数がほぼ素数である代数曲線を効率的に探索し、従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることを可能にするものである。ここで、パラメータa、bは曲線の複雑さの程度を表す。

【００２３】

$\alpha Y^{a} + \beta X^{b} + 1 = 0$という形の定義方程式をもつ、位数qの有限体$F_q$上の代数曲線を$C(q, \alpha, \beta)$とおく。代数曲線$C(q, \alpha, \beta)$に対しては、そのL関数がヤコビ和を用いて記述されることを用いて、そのヤコビアン群の位数を設計することができるのである。以下簡単のため、$q := p$（pをqとおく）は素数であり、$p \equiv 1 \bmod \mathrm{LCM}(a, b)$とする（LCMは最小公倍数）。また、1の原始ab乗根をζとおく。素数pは円分体$Q(\zeta)$において、m個の素イデアルP_1、P_2、．．．．、P_mに完全分解する。ここで、mは、法abの既約剰余類の個数である。

【００２４】

有限体F_pの乗法群F_p^{*}の生成元wを固定し、(p-1)sが整数となる有理数sに対して、F_p^{*}の指標χ_sを$\chi_s(w) = \exp(2\pi is)$（iは虚数）によって定義する。$\chi_s(0) = 0$（s: 整数でないとき）、$=1$（s: 整数のとき）として、定義域を$F_p$全体に拡張する。整数 $l=1, 2, ..., a-1$および整数 $m=1, 2, ..., b-1$に対して、$j_p(l, m) = \Sigma\_\{1+v_1+v_2=0\}\ \chi_{l/a}(v_1)\chi_{m/b}(v_2)$ はヤコビ和と呼ばれる。ここで、v_1、v_2は$1+v_1+v_2=0$を満たすv_1、$v_2 \in F_p$を走る。このとき、$C(p, \alpha, \beta)$のL関数$L_p(U)$は以下のようにヤコビ和を用いて表されることが知られている。

【００２５】

$L_p(U) = \Pi_{l=1,2,...,a-1,\ m=1,2,...,b-1}\ (1 + \chi_{l/a}(\alpha^{-1})\chi_{m/b}(\beta^{-1})\ j_p(l, m)\ U)$。

したがって、$C(p, \alpha, \beta)$のヤコビアン群の位数hは、

$h = L_p(1) = \Pi_{l=1,2,...,a-1,\ m=1,2,...,b-1}\ (1 + \chi_{l/a}(\alpha^{-1})\chi_{m/b}(\beta^{-1})\ j_p(l, m))$

で与えられる。よって、ヤコビアン群の位数を求めるには、ヤコビ和$j_p(l, m)$が計算できればよい。しかしながら、ヤコビ和$j_p(l, m)$を定義式に従って直接計算することは計算量的に不可能なので、次のヤコビ和に対するスティッケルバーガー要素を用いる。

【００２６】

$[\lambda]$は有理数λを超えない最大の整数を表し、$\langle\lambda\rangle$は有理数λの小数部分$\lambda-[\lambda]$を表すとする。また、σ_tは円分体$Q(\zeta)$のガロア写像$\zeta \to \zeta^{t}$を表すとす

る。群環Z[Gal(Q(ζ)| Q)]の元であるスティッケルバーガー要素ω(a、b)を、
$\omega(a, b) = \Sigma_t\ [\langle t/a\rangle + \langle t/b\rangle]\ \sigma_{-t}^{-1}$とおく。
ただし、tは、abを法とする既約剰余類の代表系を走るとする。

【００２７】

このとき、円分体Q(ζ)のイデアルとして、$(j_p(l, m)) = P^{\omega(a, b)}$が成立することが知られている。ここで、Pはpの上にある素イデアルである。上式より、$j_p(l, m)$は1の2ab乗根を除いて一意に定まる。そのうち、ab乗根分の自由度はC(p、α、β)の係数α、β $\in F_q$の自由度から得られる。

【００２８】

以上より、次のような安全な曲線C(p、α、β)の探索アルゴリズムが得られる。

安全な曲線C(p、α、β)の探索アルゴリズム
入力:ヤコビアンのビット数n
出力:p、α、β
（１）$g \leftarrow (a-1)(b-1)/2$
（２）ある n/g ビット程度の素数pに対するヤコビ和の候補jを後述のヤコビ和の候補値の計算アルゴリズムを用いて探す:
(p、j) ← {ヤコビ和の候補値の計算アルゴリズム}(n/g)。
（３）各k = 0、1、．．．．、ab に対して、
$h_k \leftarrow \Pi_{l=1,2,\ldots,a-1,\ m=1,2,\ldots,b-1}\ (1 + (-\zeta)^k\ j)$
（４）{ h_0、h_1、．．．．、h_{ab} }にほぼ素数である h_k があるかどうかを調べる。なければ、（１）へ戻る。あれば、$h := h_k$ とする。
（５）ζ_a、ζ_b をそれぞれ F_p における1のa乗根、b乗根とする。各 l = 0、1、．．．．、a-1 および各 m = 0、1、．．．．、b-1 に対して、曲線$C(p, \zeta_a^{\ l}, \zeta_b^{\ m}): \zeta_a^{\ l}\ y^a + \zeta_b^{\ m}\ x^b + 1 = 0$ のヤコビアン群のオーダーが h に等しいかどうか調べる。等しければ、p、$\alpha = \zeta_a^{\ l}$、$\beta = \zeta_b^{\ m}$ を出力して終了する。そのような l、m がなければ、（２）へ。
上で用いた、ヤコビ和の候補値の計算アルゴリズムでは、前記のスティッケルバーガー要素$\omega(a, b) = \Sigma_t\ [\langle t/a\rangle + \langle t/b\rangle]\ \sigma_{-t}^{-1}$ を用いて、ヤコビ和の候補

値を求める。

ヤコビ和の候補値の計算アルゴリズムは以下のようである。

入力:ビット数m、

出力:p、j、

（１） $\omega \leftarrow \Sigma_t (\langle t/a\rangle + \langle t/b\rangle)\sigma_{-t}^{-1}$、

（２） $\gamma_0 = \Sigma_{l=0}^{m-1} c_l \zeta^l$ $(-10 < c_l < 10)$ をランダムに生成。

（３）各 i = 1、2、．．． に対して、

$\gamma \leftarrow \gamma_0 + I$、

$p \leftarrow \mathrm{Norm}_{Q(\zeta)|Q}(\gamma)$、

p が約 m ビットより小さいか？、

yes → continue、

p が約 m ビットより大きいか？、

yes → （２）へ、

p が素数か？

no → continue、

（４） $j \leftarrow \gamma^{\omega}$ 、 p および j を出力して終了。

【００２９】

次に、本発明の第１の実施の形態について図面を参照して詳細に説明する。

【００３０】

図１は、本発明の第１の実施の形態を示すブロック図である。

図１を参照すると、本発明の第１の実施の形態は、スティッケルバーガー要素計算装置１１と、ヤコビ和候補値計算装置１２と、位数候補値計算装置１３と、安全性判定装置１４と、パラメータ決定装置１５と、メモリ１６と、入力装置１７と、出力装置１８と、中央処理装置１９とから構成される。

【００３１】

また、メモリ１６は、a記憶ファイル１６１、b記憶ファイル１６２、ω記憶ファイル１６３、j記憶ファイル１６４、H記憶ファイル１６５、h記憶ファイル１６６、p記憶ファイル１６７、および、n記憶ファイル１６８を含む。

【００３２】

以下では、円分体Q(ξ)における代数的数の四則演算、およびノルム$N_{Q(\xi)|Q}$の演算、および円分体Q(ξ)に対するガロア群G(Q(ξ)| Q)の作用の演算、および整数環Z係数のガロア群G(Q(ξ)| Q)上の群環Z[G(Q(ξ)| Q)]における加法および乗法演算に関しては、既知の手法を用いるものとする。

【００３３】

次に、本発明の第１の実施の形態の動作について説明する。
図２は、スティッケルバーガー要素計算装置１１の動作を示すフローチャートである。
図３は、ヤコビ和候補値計算装置１２の動作を示すフローチャートである。
図４は、位数候補値計算装置１３の動作を示すフローチャートである。
図５は、パラメータ決定装置１５の動作を示すフローチャートである。

【００３４】

曲線の複雑さの度合いを指定する2つの異なる素数a=3、b=7、および使用したい暗号鍵のサイズn=160が入力装置１７から入力された場合について説明する。入力されたa、bは中央処理装置１９を介してそれぞれa記憶ファイル１６１、b記憶ファイル１６２に一時的に記憶される。また、以下の記述において現れる変数は、メモリ１６に格納される。

【００３５】

次に、スティッケルバーガー要素計算装置１１が、図２に示す処理にしたがって、a記憶ファイル１６１、b記憶ファイル１６２よりa=3、b=7を取得して以下のように動作する。

【００３６】

図２のステップＳ２１において、変数Lにa・b = 3×7=21を法とする既約剰余類の代表系{1、2、4、5、8、10、11、13、16、17、19、20}が格納される。

【００３７】

次に、図２のステップＳ２２において、変数L={1、2、4、5、8、10、11、13、16、17、19、20}に含まれる各整数tに対して、例えば、t=1のとき、[<1/3>+<1/7>] = [1/3+1/7] = [10/21] =0なので、変数mに0が格納され、$-1^{-1} \equiv -1 \equiv 20 \bmod 21$なので、変数sに20が格納され、$0\times\sigma_{20} = 0$なので、変数$\lambda_1$に0が格納され

る。

【００３８】

他のtについても同様にして、変数λ_2に$[\langle 2/3\rangle+\langle 2/7\rangle]=[2/3+2/7]=[20/21]=0$なので0が、変数$\lambda_4$に$[\langle 4/3\rangle+\langle 4/7\rangle]=[1/3+4/7]=[19/21]=0$なので0が、変数$\lambda_5$に$[\langle 5/3\rangle+\langle 5/7\rangle]=[2/3+5/7]=[29/21]=1$で$(-5)^{-1}\equiv 16^{-1}\equiv 4 \bmod 21$なので$\sigma_4$が、変数$\lambda_8$に$[\langle 8/3\rangle+\langle 8/7\rangle]=[2/3+1/7]=[17/21]=0$なので0が、変数$\lambda_{10}$に$[\langle 10/3\rangle+\langle 10/7\rangle]=[1/3+3/7]=[16/21]=0$なので0が、変数$\lambda_{11}$に$[\langle 11/3\rangle+\langle 11/7\rangle]=[2/3+4/7]=[26/21]=1$で$(-11)^{-1}\equiv 10^{-1}\equiv 19 \bmod 21$なので$\sigma_{19}$が、変数$\lambda_{13}$に$[\langle 13/3\rangle+\langle 13/7\rangle]=[1/3+6/7]=[25/21]=1$で$(-13)^{-1}\equiv 8^{-1}\equiv 8 \bmod 21$なので$\sigma_8$が、変数$\lambda_{16}$に$[\langle 16/3\rangle+\langle 16/7\rangle]=[1/3+2/7]=[13/21]=0$なので0が、変数$\lambda_{17}$に$[\langle 17/3\rangle+\langle 17/7\rangle]=[2/3+3/7]=[23/21]=1$で$(-17)^{-1}\equiv 4^{-1}\equiv 16 \bmod 21$なので$\sigma_{16}$が、変数$\lambda_{19}$に$[\langle 19/3\rangle+\langle 19/7\rangle]=[1/3+5/7]=[22/21]=1$で$(-19)^{-1}\equiv 2^{-1}\equiv 11 \bmod 21$なので$\sigma_{11}$が、変数$\lambda_{20}$に$[\langle 20/3\rangle+\langle 20/7\rangle]=[2/3+6/7]=[32/21]=1$で$(-20)^{-1}\equiv 1^{-1}\equiv 1 \bmod 21$なので$\sigma_1$が、それぞれ格納される。

【００３９】

次に、図２のステップＳ２.３において、各変数λ_1、λ_2、λ_4、λ_5、λ_8、λ_{10}、λ_{11}、λ_{13}、λ_{16}、λ_{17}、λ_{19}、λ_{20}に記憶された全データの総和$\omega=\sigma_4+\sigma_{19}+\sigma_8+\sigma_{16}+\sigma_{11}+\sigma_1$が計算される。ここでの総和は、群環$Z[G(Q(\xi)|Q)]$における総和であり、各$\sigma_i$をシンボルとみなし、各$\sigma_i$ごとの係数の総和を意味する。演算結果である$\omega$は中央処理装置１９を介して、$\omega$記憶ファイル１６３に一時的に記憶される。

【００４０】

次に、ヤコビ和候補値計算装置１２が、a記憶ファイル１６１、b記憶ファイル１６２、n記憶ファイル１６８、ω記憶ファイル１６３から、a=3、b=7、n=160、$\omega=\sigma_4+\sigma_{19}+\sigma_8+\sigma_{16}+\sigma_{11}+\sigma_1$を取得して、図３に示す処理にしたがって、以下のようにしてヤコビ和の候補値jを演算する。

【００４１】

まず、図３のステップＳ３１において、変数ξに、ab=21なので、1の原始21乗根を格納し、変数mに、$2n/(a-1)(b-1)=26.6...$なので、27を格納する。

【００４２】

次に、図３のステップＳ３２において、変数γ_0に円分体$Q(\zeta)$のランダム整数を以下のようにして格納する。変数γ_0を0に初期化し、t=0に対し、乱数$r_0 = -2$を発生し、γ_0に$r_0 \zeta^0 = -2$を加え、$\gamma_0=-2$とし、t=1に対し、乱数$r_1 = 2$を発生し、γ_0に$r_1 \zeta^1 = 2\zeta$を加え、$\gamma_0 = -2 + 2\zeta$とし、以下同様の操作をt=11まで繰り返して、$\gamma_0 = -2 + 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$を得る。

【００４３】

次に、図３のステップＳ３３において、各整数i=0、1、2、．．．に対して、以下の操作を行う。i=0に対し、変数γに$\gamma_0 + 0$を格納し、$\gamma = -2 + 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$を得て、そのノルム$N_{Q(\zeta)|Q}(\gamma)$を計算し、129571513を得てp記憶ファイル１６７に格納し、変数lにp=129571513のビット数29を格納し、l=29がm=27程度であることを確認し、p=129571513を既知の方法により素因数分解するとp=129571513=43×211×14281となりp=129571513は素数ではないので、i=0に対する処理を終了し、i=1に対して、同様の操作を繰り返す。本実施の形態の場合は、i=2となるまで同様の操作が続き、i=2に対し、変数γに$\gamma_0 + 2$を格納し、$\gamma = 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$を得て、そのノルム$N_{Q(\zeta)|Q}(\gamma)$を計算し、163255597を得てp記憶ファイル１６７に格納し、変数lにp=163255597のビット数28を格納し、l=28がm=27程度であり、p=163255597は素数と判定されるので(素数判定には既知の手法を用いる)、ステップＳ33の操作は終了する。

【００４４】

次に、図３のステップＳ３４において、変数γの値$2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$に、スティッケルバーガー要素$\omega = \sigma_4 + \sigma_{19} + \sigma_8 + \sigma_{16} + \sigma_{11} + \sigma_1$を作用させ、結果をj記憶ファイル１６４に格納する。

【００４５】

すなわち、$j = \sigma_4(\gamma)\sigma_{19}(\gamma)\sigma_8(\gamma)\sigma_{16}(\gamma)\sigma_{11}(\gamma)\sigma_1(\gamma)$
$= -11346 + 4158\zeta + 9337\zeta^2 - 10930\zeta^3 + 3060\zeta^4 + 11132\zeta^5 - 1408\zeta^6 -$

$10000\zeta^{7} + 7506\zeta^{8} + 1237\zeta^{9} - 9894\zeta^{10} + 16406\ \zeta^{11}$

となるので、j記憶ファイル１６４の内容は $-11346 + 4158\zeta + 9337\zeta^{2} - 10930\zeta^{3} + 3060\zeta^{4} + 11132\zeta^{5} - 1408\zeta^{6} - 10000\zeta^{7} + 7506\zeta^{8} + 1237\zeta^{9} - 9894\zeta^{10} + 16406\ \zeta^{11}$ となる。

【００４６】

次に、位数候補値計算装置１３が、図４に示す処理にしたがって、a記憶ファイル１６１、b記憶ファイル１６２、j記憶ファイル１６４からそれぞれa、b、jを取得し、以下のようにしてヤコビ群の位数の候補値を計算する。

【００４７】

まず、図４のステップＳ４１において、変数ζに、ab=21なので、1の原始21乗根を格納する。

【００４８】

次に、図４のステップＳ４２において、各整数k=1、．．．．、2ab=42に対して、ヤコビ和候補値jを用いて、$N_{Q(\zeta)|Q}(1 + (-\zeta)^{k}\ j)$ を計算し、結果を変数 h_k に格納する。すなわち、k=1に対して、$N_{Q(\zeta)|Q}(1 + (-\zeta)\ j)$= 18945750554224674862720917379214050968749547249577なので、変数 h_1 に18945750554224674862720917379214050968749547249577が格納され、k=2に対して、$N_{Q(\zeta)|Q}(1 + (-\zeta)^{2}\ j)$ = 18928969305265796978830941938772180777050417721949なので、変数 h_2 に18928969305265796978830941938772180777050417721949が格納される。

【００４９】

以下同様にして、変数 h_3 に18939442397757559639176586128404383479076142135761が、変数 h_4 に18935060345406437247984249590121980321244862496761が、変数 h_5 に18935622676852726684902816970612470237474541809664が、変数 h_6 に18931936903665705475581647305574444786263237069081が、変数 h_7 に18929560654771860101383318185997674116929626012889が、変数 h_8 に18939150203650250186166315242126355786799280592469が、変数 h_9 に18932675807273674693936115572103379669380378369473が、変数 h_{10} に18942309965821405414970614992239749691042375170033が、変数 h_{11} に18934229290635176830764035532046510839791719442389が、変数 h_{12} に18935834172588603026508807514961653603431968293369が、変数 h_{13}

に1893807874305394594783193213483589967896908071028１が、変数h_{14}に1893098085411469852119769234110782679684022536846１が、変数h_{15}に1892592634848212604679740819095193047360937379135３が、変数h_{16}に1893622972431433832760815599919346449291321845963３が、変数h_{17}に1893538909827848749520574028505281217094387882325３が、変数h_{18}に1893169156778154299805089652257135802737444566507３が、変数h_{19}に1893273418061092610816670360904920771618014571784９が、変数h_{20}に1893866441174372481580378459376180146157970564769３が、変数h_{21}に1893394275277010517983798947347208061647442325496９が、変数h_{22}に1891930298633577736704954026848427386190310639076９が、変数h_{23}に1893607539688527037378171176518052249740861371362１が、変数h_{24}に1892560432898459262962746519434319120659416003707３が、変数h_{25}に1892998486378841875183615626171229937208323163357７が、変数h_{26}に1892942253179364817011122833974119815009498349977６が、変数h_{27}に1893310795454152886515284880406267275316644846076１が、変数h_{28}に1893548363470548705304356359439104829933373570399３が、変数h_{29}に1892589684834006285197213669678334822112745509834９が、変数h_{30}に1893236849047520515912445393300768155574468632677７が、変数h_{31}に1892273933686444874275028153871959910323271764287３が、変数h_{32}に1893081517521734482660949237518642372469401455195７が、変数h_{33}に1892921051036040622605765937247223088517542107700９が、変数h_{34}に1892696732793673017825053788486213781518871814067３が、変数h_{35}に1893406376327212645062378760023384352739640081243７が、変数h_{36}に1893912055976187680105429250688170088541528770104１が、変数h_{37}に1892881631571062353008946060760879733708180063247３が、変数h_{38}に1892965653857098272043807280965207220385757194178９が、変数h_{39}に1893335293386217660633123053118957918600798302424９が、変数h_{40}に1893231066327499444559974318003207993714768780512１が、変数h_{41}に1892638194570272640618262455702234411303795799170９が、変数h_{42}に1893110268178909507222967626297557734431426643361７が、それぞれ格納される。

【００５０】

最後に、位数候補値計算装置１３は、ヤコビアン群の位数の候補値として変数

h_1～変数h_{42}の内容をHとして、H記憶ファイル１６５にまとめて格納する。

【００５１】

次に、安全性判定装置１４が、H記憶ファイル１６５からHを取得し、Hに含まれる位数の候補値h_1、h_2、．．．．、h_{42}から概素数性等の安全性条件を満たす候補値hを検索し、h記憶ファイル１６６に格納する。本実施の形態では、説明を簡明にするため、安全性条件は概素数性のみを検討する。既知の素数判定法を用いると、h_{11} = 18934229290635176830764035532046510839791719442389が素数と判定され、安全性判定装置１４は、h = h_{11} = 18934229290635176830764035532046510839791719442389をh記憶ファイル１６６に格納する。

【００５２】

次に、パラメータ決定装置１５が、a記憶ファイル１６１、b記憶ファイル１６２、p記憶ファイル１６７、h記憶ファイル１６６からそれぞれa、b、p、hを取得し、図５に示す処理にしたがって動作する。

【００５３】

まず、図５のステップＳ５１において、変数ζ_3にp=163255597を法とする1の原始3乗根である127994587を、変数ζ_7にp=163255597を法とする1の原始7乗根である8342648をそれぞれ格納する。

【００５４】

次に、図５のステップＳ５２において、各整数l=1、2、3および各整数m=1、2、3、4、5、6、7に対して、以下のような処理を行う。

【００５５】

まず、l=1、m=1に対して、変数εにζ_3 = 127994587を格納し、変数ηにζ_7 = 8342648を格納し、式 $\varepsilon y^3 + \eta x^7 + 1 = 127994587 y^3 + 8342648 x^7 + 1 = 0$ で定義される代数曲線のヤコビアン群のランダムな元$\{151707017 + 104678491 x + 123646083 x^2 + 18753988 y + 87634493 x^3 + 61274336 x y + x^4$、$138799785 + 145105684 x + 584395 x^2 + 80828873 y + 34715892 x^3 + 121885874 x y + 59787844 x^4 + x^2 y$、$161162224 + 117150097 x + 100956100 x^2 + 89380061 y + 140032555 x^3 + 43367019 x y + y^2\}$を生成し、これを変数Gに格納し、変数Gに格納されている点の、ヤコビアン群におけるh=189342292906351768307

6403553204651083979171944 2389倍を計算し、計算結果である｛$133659497 + 103424746 x + 136032897 x^2 + 131029199 y + 24618867 x^3 + 114944034 x y + x^4$、 $86125426 + 125891893 x + 19568269 x^2 + 27044314 y + 80420960 x^3 + 137562092 x y + x^2 y$、 $53604112 + 65990501 x + 51269221 x^2 + 55271502 y + 7974233 x^3 + 84922220 x y + y^2$｝を変数Gに格納する。

【００５６】

変数Gの上記内容がヤコビアン群における単位元｛｝に等しくないので、次に、l=1、m=2に対して、変数εにζ_3 = 127994587を格納し、変数ηに$\zeta_7^2 = 83426482 \bmod 163255597$ = 159772073を格納し、上記の処理を繰り返す。

【００５７】

本実施の形態の場合、l=2、m=2に対して、ε=35261009、η=159772073となり、ランダムに生成された点G = ｛$4568071 + 141843715 x + 68256743 x^2 + 71903501 y + 128953783 x^3 + 10781960 x y + x^4$、 $48272788 + 45615229 x + 150692034 x^2 + 53973350 y + 11114765 x^3 + 78550130 x y + 61331354 x^4 + x^2 y$、 $117552807 + 135448907 x + 64074711 x^2 + 141058974 y + 49208246 x^3 + 93940317 x y + y^2$｝のh=1893422929063517683076403553204651083979171944 2389倍が単位元｛｝となり、パラメータ決定装置１５は安全な代数曲線のパラメータとして、p=163255597、ε=35261009、η=159772073を出力する。

【００５８】

最後に、パラメータ決定装置１５の出力したパラメータp=163255597、ε=35261009、η=159772073が出力装置１８より出力される。

【００５９】

次に、本発明の第２の実施の形態について詳細に説明する。

本発明の第２の実施の形態は、

（ａ）a記憶ファイル１６１、b記憶ファイル１６２から、それぞれ素数a、bを取得し、円のab分体におけるスティッケルバーガー要素ωを演算するスティッケルバーガー要素計算手順と、

（ｂ）前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素ωをω記憶ファイル１６３に記憶する手順と、

（ｃ）a記憶ファイル１６１、b記憶ファイル１６２、n記憶ファイル１６８、ω記憶ファイル１６３からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωを取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

（ｄ）前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶ファイル１６７、およびj記憶ファイル１６４に記憶する手順と、

（ｅ）a記憶ファイル１６１、b記憶ファイル１６２、j記憶ファイル１６４から、それぞれ素数a、素数b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

（ｆ）前記位数候補値計算手順により演算された集合HをH記憶ファイル１６５に記憶する手順と、

（ｇ）H記憶ファイル１６５から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

（ｈ）前記安全性判定手順により検索された候補値hをh記憶ファイル１６６に記憶する手順と、

（ｉ）a記憶ファイル１６１、b記憶ファイル１６２、p記憶ファイル１６７、h記憶ファイル１６６からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

を含むことを特徴とする代数曲線暗号における安全なパラメータの生成方法である。

【００６０】

次に、本発明の第３の実施の形態について図面を参照して詳細に説明する。

図６は、本発明の第３の実施の形態を示すブロック図である。

図６を参照すると、本発明の第３の実施の形態は、本発明の第２の実施の形態の各手順をコンピュータ１００に実行させるプログラムを記録する記録媒体１３０である。このプログラムは、コンピュータ１００の記憶装置にロードされ実行される。

【００６１】

【発明の効果】

本発明の効果は、従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることができ、代数曲線暗号の安全性を向上することである。

【００６２】

その理由は、$\alpha Y^{a}+\beta X^{b}+1=0$という形の定義方程式をもつ代数曲線のクラスから、そのヤコビアン群の位数がほぼ素数である代数曲線を効率的に探索することが可能となり、使用できる代数曲線の範囲が広がり、攻撃者の解読作業が分散増加するからである。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態を示すブロック図である。

【図２】

スティッケルバーガー要素計算装置の動作を示すフローチャートである。

【図３】

ヤコビ和候補値計算装置の動作を示すフローチャートである。

【図４】

位数候補値計算装置の動作を示すフローチャートである。

【図５】

パラメータ決定装置の動作を示すフローチャートである。

【図６】

本発明の第３の実施の形態を示すブロック図である。

【符号の説明】

１１　スティッケルバーガー要素計算装置

１２　ヤコビ和候補値計算装置

１３　位数候補値計算装置

１４　安全性判定装置

１５　パラメータ決定装置

１６　メモリ

１７　　入力装置

１８　　出力装置

１９　　中央処理装置

１００　　コンピュータ

１３０　　記録媒体

１６１　　a記憶ファイル

１６２　　b記憶ファイル

１６３　　ω記憶ファイル

１６４　　j記憶ファイル

１６５　　H記憶ファイル

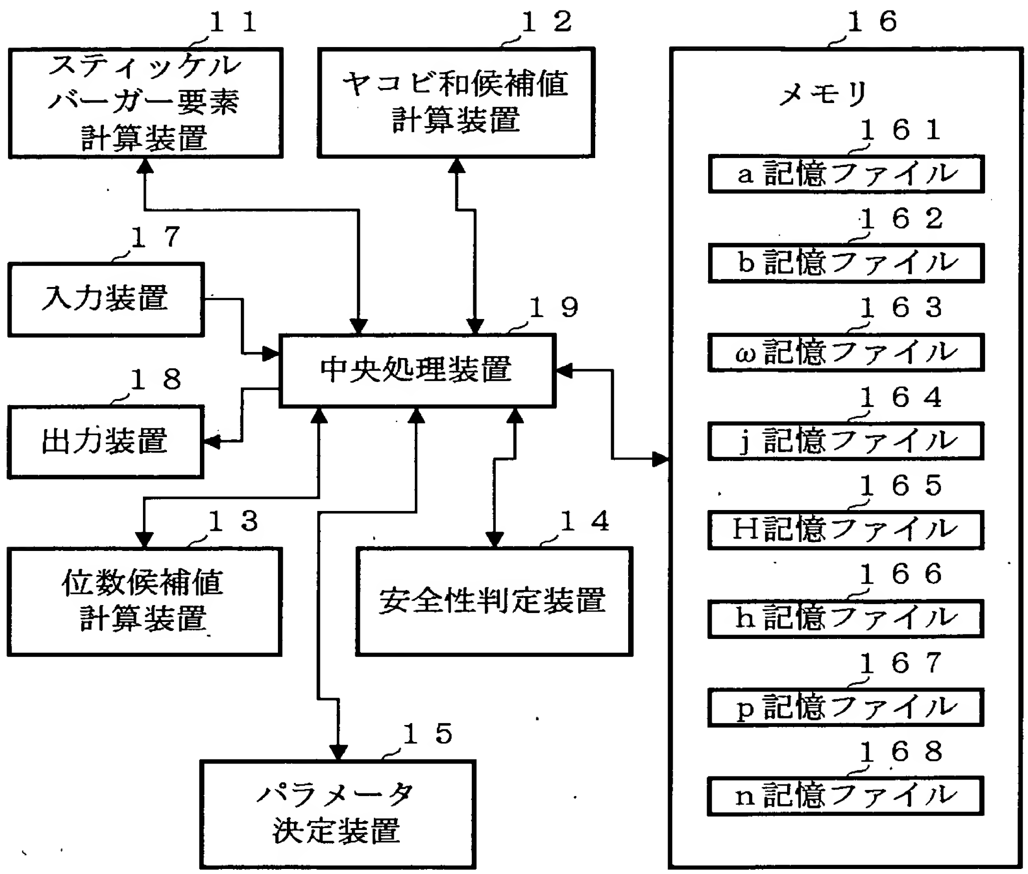
１６６　　h記憶ファイル

１６７　　p記憶ファイル

１６８　　n記憶ファイル

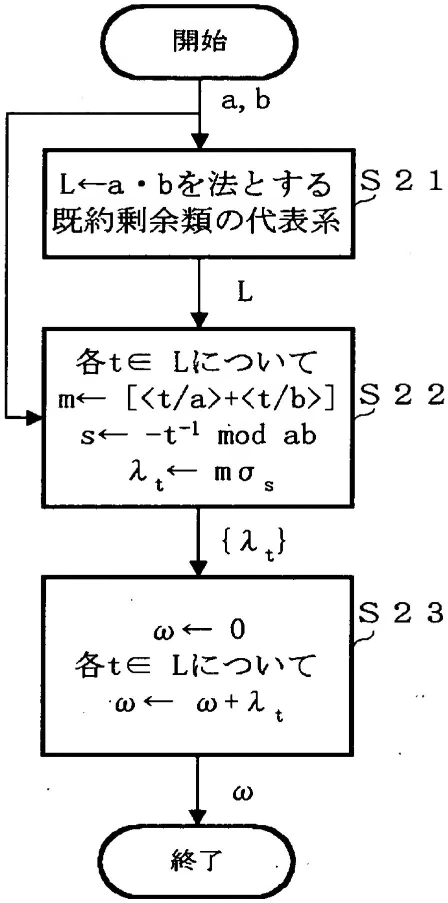
【書類名】　　図面

【図１】

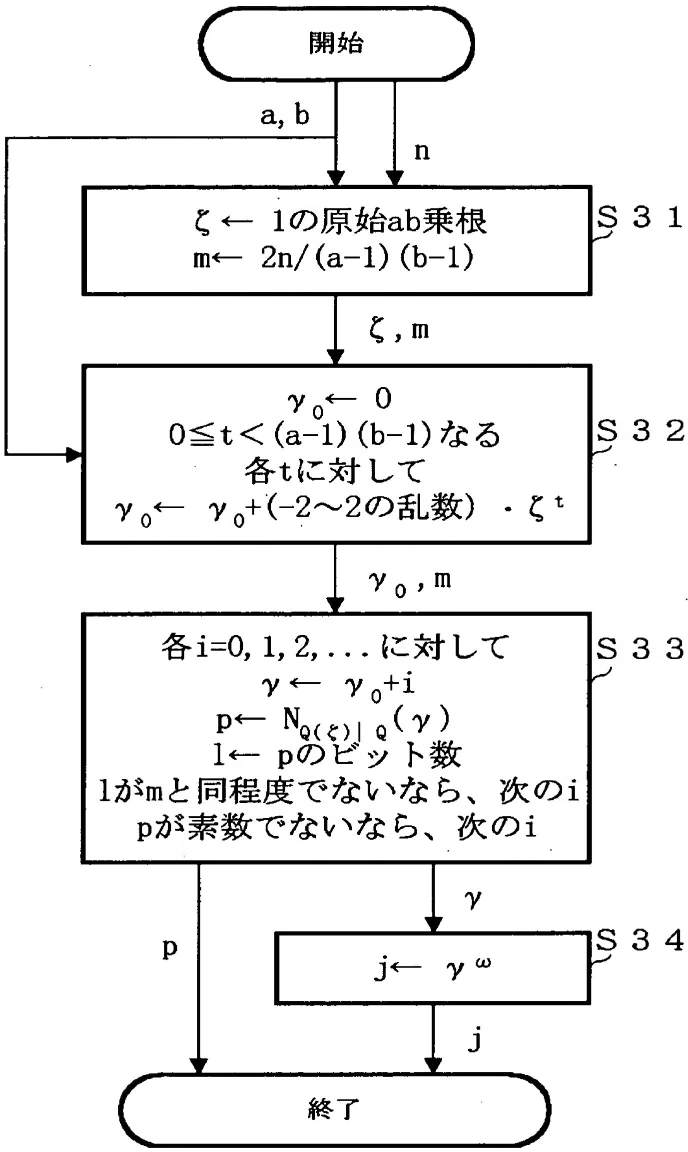


１１
スティッケルバーガー要素計算装置
１２
ヤコビ和候補値計算装置
１６
メモリ
１６１
ａ記憶ファイル
１６２
ｂ記憶ファイル
１６３
ω記憶ファイル
１６４
ｊ記憶ファイル
１６５
Ｈ記憶ファイル
１６６
ｈ記憶ファイル
１６７
ｐ記憶ファイル
１６８
ｎ記憶ファイル
１７
入力装置
１８
出力装置
１９
中央処理装置
１３
位数候補値計算装置
１４
安全性判定装置
１５
パラメータ決定装置

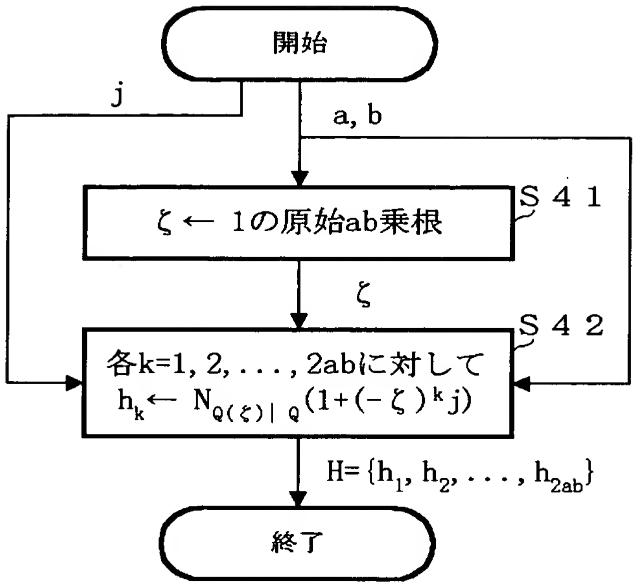
【図２】


開始
a, b
L←a・bを法とする既約剰余類の代表系
S２１
L
各t∈ Lについて
m← [<t/a>+<t/b>]
s← −t^-1 mod ab
λt← mσs
S２２
{λt}
ω← 0
各t∈ Lについて
ω← ω+λt
S２３
ω
終了

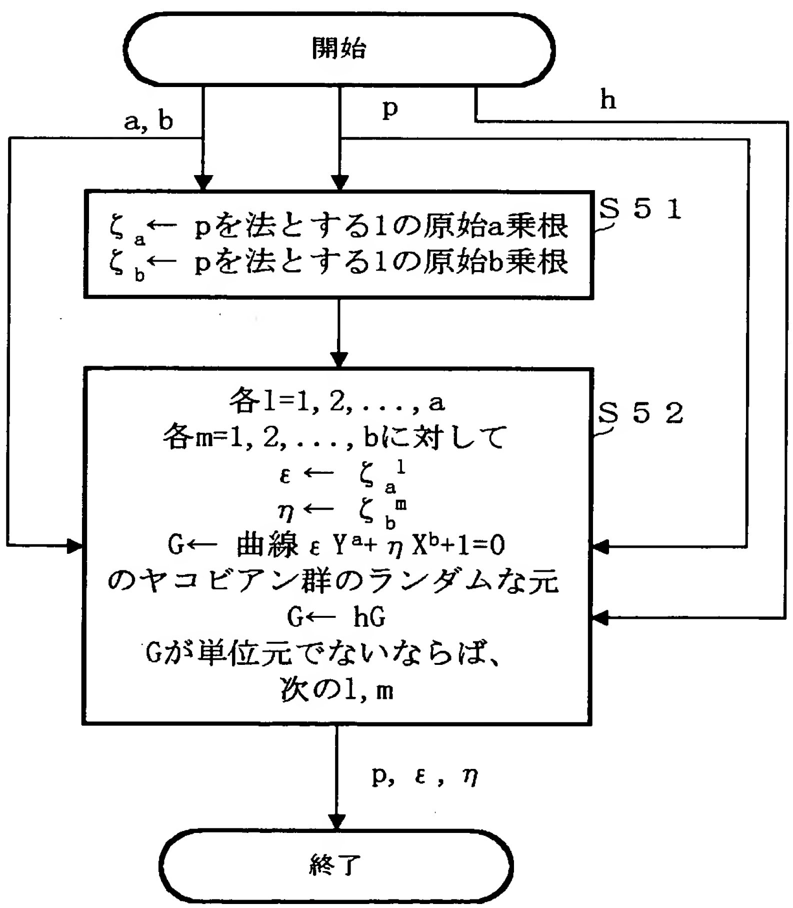
【図３】


開始
a, b
n
ζ← 1の原始ab乗根
m← 2n/(a-1)(b-1)
S３１
ζ, m
γ0← 0
0≦t＜(a-1)(b-1)なる
各tに対して
γ0← γ0+(-2～2の乱数)・ζt
S３２
γ0, m
各i=0, 1, 2, . . . に対して
γ← γ0+i
p← NQ(ζ)|Q(γ)
l← pのビット数
lがmと同程度でないなら、次のi
pが素数でないなら、次のi
S３３
p
γ
j← γω
S３４
j
終了

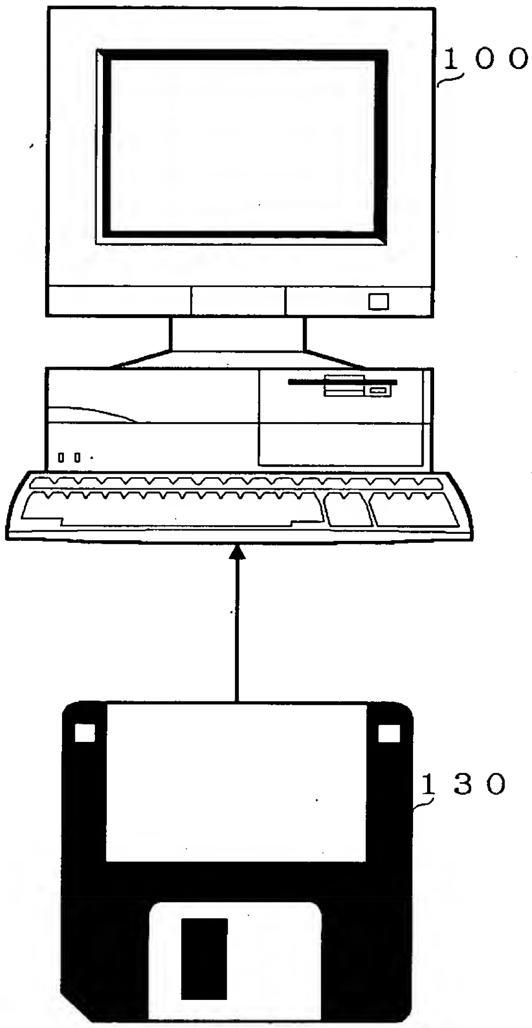
【図４】


開始
j
a, b
ζ← 1の原始ab乗根
S４１
ζ
S４２
各k=1, 2, . . . , 2abに対して
h_k← $N_{Q(\zeta)|Q}(1+(-\zeta)^k j)$
H={h_1, h_2, . . . , h_{2ab}}
終了

【図５】


開始
a, b
p
h
ζ_a← pを法とする1の原始a乗根
ζ_b← pを法とする1の原始b乗根
S５１
各l=1, 2, . . . , a
各m=1, 2, . . . , bに対して
ε ← ζ_a^l
η ← ζ_b^m
G← 曲線 $\varepsilon Y^a+\eta X^b+1=0$
のヤコビアン群のランダムな元
G← hG
Gが単位元でないならば、
次のl, m
S５２
p, ε, η
終了

【図６】



【書類名】　　　要約書

【要約】

【課題】　従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることを可能とし、代数曲線暗号の安全性を向上させる。

【解決手段】　スティッケルバーガー要素計算装置１１が、円のab分体におけるスティッケルバーガー要素ωを演算し、次に、ヤコビ和候補値計算装置１２が、素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素ωから、ヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算し、位数候補値計算装置１３が、素数a、素数b、ヤコビ和候補値jから、代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算し、安全性判定装置１４が、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索し、パラメータ決定装置１５が、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算する。

【選択図】　　　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第２４２０７５号
受付番号	５９９００８３２９２３
書類名	特許願
担当官	第七担当上席　　　　　００９６
作成日	平成１１年　８月３１日

<認定情報・付加情報>

【提出日】	平成11年 8月27日

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００４２３７〕

１．変更年月日　１９９０年　８月２９日
　　［変更理由］　新規登録
　　　住　所　東京都港区芝五丁目７番１号
　　　氏　名　日本電気株式会社